Sicherheitsanalyse und Implementierung einer hierarchischen Zugriffskontrolle für sichere Gruppenkommunikation auf Basis des chinesischen Restesatzes

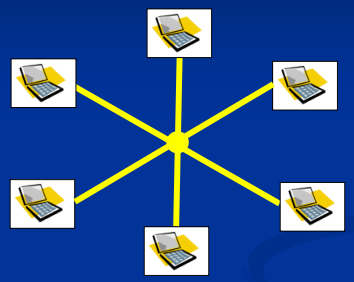
Masterarbeit von Mark Manulis

Betreuung von Prof. S. Fischer, Prof. D. Wätjen und Dipl.-Wirt.-Inf. S. Schmidt

Inhalt

- CRTHACS –
  Chinese Remainder Theorem Based Hierarchical Access Control for Secure Group Communication
  (von X. Zou, B. Ramamurthy, S. S. Magliveras auf ICICS 2001)
- Beschreibung des CRTHACS-Verfahrens
- Sicherheitsanalyse
- Implementierung + Demo

Gruppenkommunikation

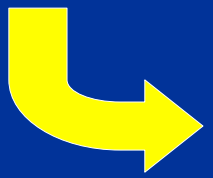


Gruppenarten:
- offene / geschlossene
- flache / hierarchische
- statische / dynamische
- anonyme / bekannte

Kommunikationsarten:
- Unicast
- Concast
- Multicast / Broadcast
- Multipeer

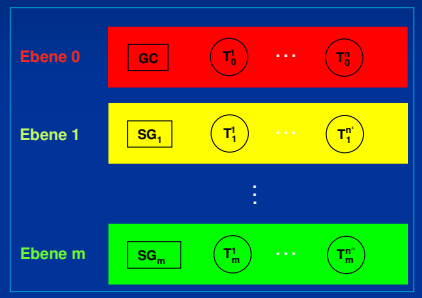
Sicherheitsanforderungen

- Angriffsziele:
  - Nachrichten
  - Gruppenmitglieder



- Anforderungen:
  - Vertraulichkeit
  - Authentizität und Integrität
  - Zugriffskontrolle
  - Unleugbarkeit

CRTHACS - Gruppe



- GC – Gruppen-Kontroller
- SG – Teilgruppen-Kontroller
- T – Gruppenmitglied

Ziel:

Verschlüsselte Nachrichten können nur von den Mitgliedern dechiffriert werden, die sich in der Hierarchie auf der gleichen oder höheren Ebene befinden.

Initialisierung 1

- Jedes Objekt hat ein Schlüsselpaar und eine eindeutige ID

GC	SG_i	T_j
P_{GC}, S_{GC}	P_i, S_i	p_j, s_j
ID_{GC}	ID_i	id_j

- Initalisierung des Gruppen-Kontrollers GC

begin

1. Bestimme die Anzahl der Teilgruppen m.
2. Generiere $N_0, N_1 \ldots, N_m$, die paarweise relativ prim sind.

end;

Initialisierung 2

- Jede Teilgruppe besitzt: $P_i, S_i, K_i, N_i, COM\_CRT_i, \mathbf{N}_i$
- Initialisierung eines Teilgruppen-Kontrollers SG_i:

1. SG_i authentifiziert sich gegenüber dem GC.
2. SG_i wählt den Gruppen-Kommunikationsschlüssel K_i und sendet $E_{P_{GC}}(D_{S_i}(K_i))$ an GC.
3. GC dechiffriert K_i durch Bildung von $E_{P_i}(D_{S_{GC}}(E_{P_{GC}}(D_{S_i}(K_i))))$ und bestimmt für die Teilgruppe G_i alle Teilgruppen $G_{i_1}, \ldots, G_{i_k}$ mit $G_i <_H G_{i_j}, j \leq k$ und $j, k \in \mathbb{N}$. GC bestimmt zunächst
$$\mathbf{N}_i = N_{i_1} \cdot N_{i_2} \cdots N_{i_k},$$
löst dann das folgende Gleichungssystem mit dem chinesischen Restealgorithmus (Kapitel 2.8) auf und bestimmt den CRT-Schlüssel COM_CRT_i:
$$\begin{aligned} COM\_CRT_i &= E_{P_{i_1}}(K_i) \bmod N_{i_1} \\ COM\_CRT_i &= E_{P_{i_2}}(K_i) \bmod N_{i_2} \\ &\vdots \\ COM\_CRT_i &= E_{P_{i_k}}(K_i) \bmod N_{i_k} \end{aligned}$$
Anschließend sendet GC
$$E_{P_i}(D_{S_{GC}}(N_i, COM\_CRT_i, \mathbf{N}_i))$$
an SG_i.
4. SG_i dechiffriert $(N_i, COM\_CRT_i, \mathbf{N}_i) = E_{P_{GC}}(D_{S_i}(E_{P_i}(D_{S_{GC}}(N_i, COM\_CRT_i, \mathbf{N}_i))))$.

Initialisierung 3

- Initialisierung eines Gruppenmitglieds T_j:

begin

1. T_j authentifiziert sich gegenüber SG_i und GC.
2. SG_i sendet T_j
$$E_{p_j}(D_{S_i}(P_i, S_i, K_i)).$$
3. GC sendet T_j
$$N_0, E_{p_j}(D_{S_{GC}}(N_i, COM\_CRT_i, \mathbf{N}_i)).$$
4. T_j dechiffriert die empfangenen Nachrichten.

end;

Gruppennachrichten senden

begin

1. T_j chiffriert die Nachricht M mit einem symmetrischen Verfahren und dem Gruppenschlüssel K_i zu $E_{K_i}(M)$.
2. T_j berechnet den MAC-Wert $MAC_{K_i}(E_{K_i}(M))$ mit einer MAC-Funktion.

$$CRT_i = COM\_CRT_i \bmod \mathbf{N}_i$$
$$CRT_i = D_{s_j}(MAC_{K_i}(E_{K_i}(M))) \bmod N_0$$

   mit dem CRA. Dabei bezeichnet D_{s_j} die asymmetrische Signierung mit dem geheimen Schlüssel s_j des Teilnehmers.
3. T_j führt die Funktion **Multicast**$(id_j, CRT_i, E_{K_i}(M))$ aus, die den Tripel an die Multicast- bzw. Broadcastadresse des Netzes und damit auch an alle Gruppenmitglieder sendet .

end;

Gruppennachrichten empfangen

begin

1. Der Teilnehmer $T_{j'}$ empfängt das Tripel $(id_j, CRT_i, E_{K_i}(M))$;
2. $T_{j'}$ berechnet $CRT_i \bmod N_0 = D_{s_j}(MAC_{K_i}(E_{K_i}(M)))$;
3. $T_{j'}$ bestimmt $E_{p_j}(D_{s_j}(MAC_{K_i}(E_{K_i}(M))))$ und erhält damit $MAC_1 = MAC_{K_i}(E_{K_i}(M))$;
4. **if** $T_{j'} \in G_i$ **then**
   $K_i = K_{j'}$;
   else if $T_{j'} \in G_{i_j}$ mit $G_i <_H G_{i_j}$ **then**
   $CRT_{i_j} = CRT_i \bmod N_{i_j}$;
   $K_i = D_{S_{i_j}}(CRT_{i_j})$;
   else break;
5. $MAC_2 = MAC_{K_i}(E_{K_i}(M))$;
6. **if** $MAC_1 = MAC_2$ **then**
   $M = D_{K_i}(E_{K_i}(M))$;
   else break;

end;

Zusätzliche Eigenschaften

- Unabhängiges Schlüsselschema
- Verdeckung der Hierarchie
- Anonymität des Empfängers
- Dynamisches Verhalten

Sicherheitsanalyse - Vertraulichkeit

- Vertraulichkeit ist durch die symmetrische Verschlüsselung mit K gewährleistet.
- K ist bestimmbar aus abgefangenen Nachrichten der Initialisierungsprotokolle und dem Kenntnis des geheimen RSA-Schlüssels eines Empfängers.
- Risiken:
  - Verwendung von K bei Bildung des MAC-Werts
  - Unabhängiges Schlüsselschema → Zwei gleiche Schlüssel möglich

Sicherheitsanalyse - Nachrichtenauthentizität

- Authentizität ist durch die Bildung des signierten MAC-Werts gewährleistet. Die Integrität der Nachricht durch die Verschlüsselung.
- Angriff mit COM_CRT_i , $\mathbf{N_i}$, K_i und s_j
- Reduktion der notwendigen Parameter
  - CRT_i mod $\mathbf{N_i} = COM\_CRT_i$
  - Andere Richtung: COM_CRT_i → $\mathbf{N_i}$ möglich [Abs. 3.2.2]
  - Von 4 bis auf 1 Parameter je nach Ausgangssituation

Sicherheitsanalyse - Hierarchie

- Verdeckung der Hierarchie wird durch die geheimen N_i der Teilgruppen bzw. durch die schwierige Primfaktorzerlegung von $\mathbf{N_i}$ gewährt.
- N_i ist bestimmbar aus abgefangenen Nachrichten der Initialisierungsprotokolle und dem Kenntnis des geheimen RSA-Schlüssels eines Empfängers.
- Collusion-Angriff [Abs. 3.2.3] mit r Mitgliedern unterschiedlicher Teilgruppen mit einer Wahrscheinlichkeit von $p(N_i) = h / (H-r)$

H - Gesamte Anzahl der Teilgruppen r - Anzahl der Partner-Teilgruppen h - Anzahl der höheren Teilgruppen

Sicherheitsanalyse - Unleugbarkeit

- Sendevorgang [Abs. 3.2.4] :
  - Es muss eine Verbindung zwischen der gesendeten Nachricht und dem Sendezeitpunkt geben
- Empfangsvorgang [Abs. 3.2.4]:
  - Zuverlässige Übertragung notwendig → kein IP-Multicast
  - Entschlüsselung über die Hierarchiefeststellung mit Hilfe von Kontrollern nachweisbar

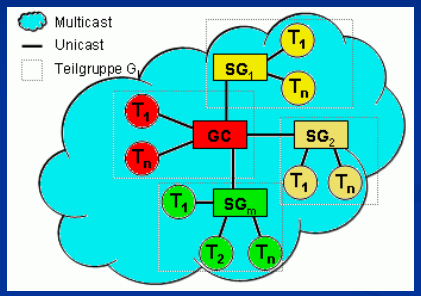
Sicherheitsanalyse - Dynamisches Verhalten

- Das dynamische Verhalten ist ineffizient, weil die Wiederherstellung von Sicherheitskriterien einen Aufwand erfordert, der beinahe dem Initialisierungsaufwand der Gruppe gleich kommt.

  [Abs. 3.2.5]

Implementierung des CRTHACS-Communicators

- Netzwerkverbindungen innerhalb der CRTHACS-Gruppe:



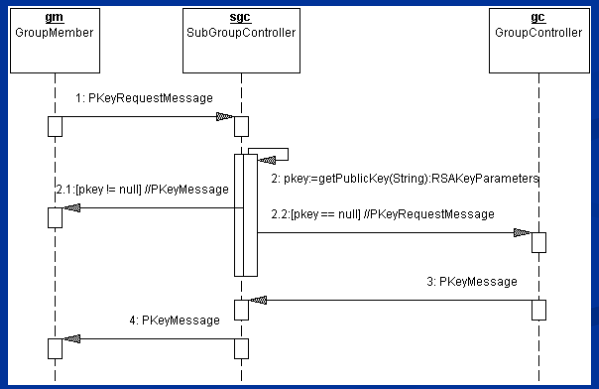
- Konfigurationsdateien werden mit *CRTHACS-Configurator* erzeugt:
  - group-id-config.xml
  - gc-id-config.xml, sgc-id-config.xml und gm-id-config.xml

Implementierung des CRTHACS-Communicators 2

- Pakete des *CRTHACS-Communicators*:
  - crthacs
  - crthacs.com
  - crthacs.com.messages
  - crthacs.com.protocol
  - crthacs.crypto
  - crthacs.gui
- Nachrichten werden in XML-Format versendet und mit einem DOM-Parser geparst. Alle Nachrichtenklassen implementieren das gemeinsame Interface NetworkMessage.

Implementierung des CRTHACS-Communicators 3

- PKI wird durch den Gruppen-Kontroller simuliert, deshalb sind Public-Key-Anfragen nötig:



Vorführung

- Installieren über *setup.jar*
- Start CRTHACS-Communicator über *crthacscommunicator.jar*

Danke für die Aufmerksamkeit